9-2012

Reputation as Public Policy for Internet Security

Leigh L. Linden

John S. Quarterman

Qian TANG
Singapore Management University, QIANTANG@smu.edu.sg

Andrew B. Whinston

Reputation as Public Policy for Internet Security

TPRC 2012

John S. Quarterman
Quarterman Creations
Email: antispam@quarterman.com
Rev: 1.10 2012/08/17 19:48:41

Leigh L. Linden
Department of Economics,
University of Texas at Austin
Email: leigh.linden@austin.utexas.edu

Qian Tang and
Andrew B. Whinston
Center for Research in Electronic Commerce
University of Texas at Austin
Email: abw@uts.cc.utexas.edu

***Abstract*—Insufficient resource allocation causes an Internet information security (infosec) problem that public policy could improve. Lack of transparency lets organizations avoid addressing internal risks, leaving vulnerabilities that are exploited by botnets, threatening information security of other Internet participants. Their protection provides no economic benefit to the firm, so this negative externality causes underinvestment in infosec. Public policy could provide a partial solution by adding incentives for organizations to have well-configured infosec. Specifically, mandatory reporting of security issues plus presenting this information to the public, can impose shame and fame on organizations through publicity and peer influence by comparison with major competitors. Outbound spam is a prominent symptom of poor infosec that this project uses as a proxy for overall security, mapping anti-spam blocklist IP addresses to organizations [1]. Selected top outbound spam rankings publicized through SpamRankings.net have already produced positive pilot test results. Next we use field experiments to test the effects of information disclosure and the relative effectiveness of different information presentations.**

As the first of two objectives, we determine whether public ranking of spam can be an effective mechanism for encouraging firms to reduce outbound spam. Second, we explore the most effective ways of presenting information to the public to improve infosec. Our study serves as an assessment for the public policy of mandatory information disclosure. We use field experiments to aggregate company information within and between industries and analyze the results of presenting such information to the public. Field experiments have been used extensively in the analysis of public policy programs [2] [3]. The experiments include design of an information system for public information disclosure and presentation to get public attention, to observe reactions, and to analyze the underlying mechanisms. This information system design can be extended to other problems to provide incentives for the decision makers of externality problems, such as pollution, energy saving, etc. A public information system enables inferring internal infosec based on observed outcome, and thus makes such information transparent and induces reputation for the decision makers: shame for producing negative externalities or fame for fixing or preventing them. Reputation internalizes externalities, encouraging decision makers to take socially optimal behavior.

Because of the positive pilot test results, we propose conducting a full-scale randomized controlled trial based on the SpamRankings.net initiative. The purpose of a randomized controlled trial is to experimentally create individual research groups that are generally similar except that the groups receive different experimental treatments. So any differences that arise between the research groups subsequent to the treatments are due to the respective treatment. Randomized experiments thus avoid selection bias, producing high internal validity.

For two full-scale experiments, we will identify a sample of companies by geographic units for which we have outgoing spam data, and randomly assign the companies by geographic unit to different groups. In the first experiment, we will randomly assign the companies to one of two groups: a treatment group whose spam statistics will be widely publicized and a control group without publicizing any spam information. This initial evaluation can examine whether the proposed policy can induce firms to reduce spam. Assuming success of the first experiment, the second will explore the most effective policy intervention, by randomly assigning company groups to different information presentations including absolute spam volume, ranking per country, and ranking per industry, to see what granularity of peer comparison has the most effect.

This is the first publication of the details and the behavioral economics context of these experiments. Supported by NSF grant no. 0831338; the usual disclaimers apply.

I. Introduction

Although various technical tools are available, the fundamental problem with improving Internet security is the lack of incentives to adopt these tools while containing their costs. Good information security (infosec) is not just techniques: it is also procedures and processes. 90 percent of cyber attacks could be avoided with "good hygiene," [4]. The problem is that as long as ESPs act individually and think no one can see their infosec, they have no incentive to implement the techniques or organize them with procedures and processes.

This paper describes field experiments using Internet operational data to study new economic and policy incentives for electronic mail service providers (ESPs) and other Internet participants to take responsibility and act collectively to improve Internet security. These experiments may justify policies for other infosec reporting, for further infosec improvement.

Towards the goal of improved security we use a proxy: outbound spam (bulk unsolicited email), [5]. Spam is a sneeze for infosec disease, because spam is typically sent via botnets or other malware that infests organizations due to poor infosec.

The purpose of the project is to use available information on the quantity of spam emitted by individual organizations to encourage these organizations to adopt stronger infosec measures by publicizing the data. Economic theory predicts that by publicizing such information firms will come under pressure to change their policies through several mechanisms, such as peer pressure, more information about the magnitude of the problems existing in their networks, or the threat of customers

switching to competitors with better security. We intend to test whether or not a program that simply publicizes the existing information (despite the limitations of this information) on the quantity of spam released by the companies can cause them to change their behavior. More generally, we aim to demonstrate the feasibility of using randomized controlled trials to explore organizational infosec decision processes.

Just as other diseases might not cause sneezes, organizations that react to these new incentives and fix their spam problem might still have other security problems. Organizations could use the same sorts of technology they already use to filter inbound spam [6] to filter outbound spam. Nothing we propose is a panacea for all infosec problems. However, preliminary experiments thus far indicate that ranked organizations do prefer to try to fix their underlying infosec problems. We will study how much this is true as part of the project.

Many organizations consider outbound spam to be somebody else's problem and thus ignore it, minimizing infosec expenditure in favor of profits [7], [8], [9]. The same unaddressed vulnerabilities that let spammers in are often exploited to threaten the security and interests of other Internet participants, whose protection provides no economic benefit to the firm. This creates what economists refer to as a negative externality, resulting in underinvestment in infosec.

Public policy could provide a partial solution to this externality by providing additional incentives for organizations to have well-configured infosec. Specifically, mandatory reporting of security issues plus presenting this information in a relative way (as rankings) to the public, can impose shame and fame on organizations through publicity and peer influence by comparison with major competitors.

We have obtained spam data for the entire Internet from blocklists (lists of IP addresses known to send spam). Later we will add experiments using phishing data. Decreasing spam or phishing for treated organizations are merely steps towards or byproducts of the actual goal, which is ongoing infosec improvement through improved incentives.

Reputational incentives through rankings such as in SpamRankings.net can provide transparency that enables ESPs to see what infosec works and for competitors and customers to see that an ESP's infosec is working. Such improved infosec resource allocation may be tied to marketing and sales through the effects shown in rankings. Organizational infosec may thus convert from a cost center to a profit center by retaining or attracting customers. With measurement, an enterprise can take more control over its use of the Internet [10], [11], [12].

The project team daily collects data on outbound spam volume observed for IP addresses and maps these IP addresses to Autonomous Systems (ASes) and soon also to their owning organizations. The core of the project is a field experiment to test the impact of information disclosure on outbound spam and the relative effectiveness of different information presentations including absolute volume and relative rankings.

As pilot tests, selected top outbound spam rankings published through SpamRankings.net have already produced tentative positive results with medical and other organizations.

II. Methods

A standard full-scale randomized controlled trial (RCT) normally requires on the order of 2,000 units to randomize for optimal power of experimental results. Such numbers of units are difficult for rankings such as those in SpamRankings.net, because there are fewer than 2,000 countries in the world. Nonetheless, we have an opportunity to apply RCT in some form to data that may never have been studied in that way; data that cover the whole world every day. Such an attractive opportunity may require some modifications of approaches used for other data.

A. Geographical scope and unit size

Using smaller geographical units than countries would seem likely to produce more units for randomization, but the smaller the geographic unit, the less spam. Units down to the Metropolitan Statistical Area (MSA) or city level might seem convenient. (See also §*II-G4 Ranking levels* about organizational, ASN, or netblock levels.) For example, medical organizations in Atlanta, Boston, and Shanghai. However, a rather solid preliminary observation is that we never see spam from most ASNs in the world. Specifically, we usually do not observe more than a dozen or so spamming medical organizations worldwide, so there is no reason to expect that individual cities will have enough such organizations for randomization per city to work.

The issue is not precision or accuracy or difficulty of assigning geographic locations for the ASNs. The issue is that because most ASNs do not spam, the smaller the geographical area, the less spam can be expected to be seen from it.

For a few large organizational types, such as ISPs or hosting companies, there may be enough ASNs and spam for more local geographical areas to work, and we will explore that possibility. However, for our main initial experiments we focus on countries as the basic geographical unit.

Randomizing selection of ASNs within a country to publicize would produce published lists of ASNs that weren't really rankings, since some ASNs that would have enough observed spam volume to appear would be in the control group and would not be published. So it is more feasible to use countries as a whole as the unit of randomization. Fortunately, statistical techniques have been developed to deal with clustered data.

B. Clustered RCT

Clustered randomized controlled trials are increasingly popular in medical studies [13]. In cluster assignment of samples into different groups, the essential sample size becomes the number of clusters instead of the number of individuals. However, medical studies do not typically require thousands of groups to cluster. One medical study of heart failure management involved 197 individuals (56 in the intervention group and 95 in the control group) [14]. The Consolidated Standards of Reporting Trials (CONSORT) have been extended to add a few points for clustered randomized trials [15].

Clustered RCTs have been used outside hospitals in the field, such as in a recent study of immunization of children

in India [16] that is somewhat analogous to our experiments. The individual participants in that study were 1640 children in 134 villages, and the villages were the units of randomization. 1640 is far less than the number of ASNs for which we have data. 134 is less than the 200+ countries for which we have data, and in the same range as the number of countries for which we have many ASNs.

One reason for the popularity of medical clustered RCTs is that medical subjects naturally cluster (in wards, or by treatments other than those being studied, etc.), and it is important to take such clustering into account in statistical analysis [13]:

> Members of a cluster will be more like one another than they are like members of other clusters and we need to take this into account in the analysis, and preferably the design, of the study. Methods which ignore clustering may mislead, because they assume that all subjects provide independent observations.

Similarly, organizations on the Internet do cluster in countries, so our analysis will take that fact into account. Meanwhile, we have huge advantages that medical trials mostly do not: ongoing daily data and worldwide coverage. A relatively small clustered RCT will serve as a starting point. If results are positive, they will motivate more extensive experiments.

C. Selection and description of sample

In our study, the organizations are clustered by countries. The outcome evaluations are based on comparing organizations in the treatment countries to organizations in other similar countries. For the purpose of this study, organizations within one country need to be ranked together. So we could not do treatment selection at the organization level. Therefore, we nest ASNs within countries and assign countries as clusters to the treatment condition. While clustered assignment is more practical and has been extensively used by existing studies, its disadvantage is that the effective sample size becomes much smaller: it is the number of clusters rather than individuals.

1) Correlation within country: Because outbound spam may be correlated within country as a result of common policies and regulations, failure to correct the standard errors could result in an overestimate of the treatment effects [17] [18]. We therefore need to cluster the standard errors at the country level (the level of treatment assignment) in all of the above models. Cluster-robust standard errors permit heteroskedasticity and within-cluster error correlation, but can still over-reject with few (five to thirty) clusters [19]. So with few countries in the data, we need to further bootstrap the strand errors to derive more precise estimation. Cameron et al. (2008) showed that wild cluster bootstrap-t procedure performs better than other bootstrap procedures (including pairs cluster bootstrap-t, residual cluster bootstrap-t, and all bootstrap-se methods) when the number of clusters is small.

There is reason to suspect correlation of outbound spam within countries could be limited, similarly to what Banerjee and Duflo noted about economic growth [20]:

> The key fact is the enormous heterogeneity of rates of return to the same factor within a single economy, a heterogeneity that dwarfs the cross-country heterogeneity in the economy-wide average return.

It is well-known that national legal attempts to stop spam or to improve infosec have had limited effect. See for example the way snowshoe spam is spreading beyond the U.S. [21], or how the recent takedown of the Grum botnet [22] (which itself infested organizations in multiple countries) was followed by an expansion of spam traffic from the Festi botnet that pushed Saudi Arabia and Turkey into the top 10 spam-spewing countries worldwide and made India number one [23].

2) Spam distribution by country and ASN: Our database has collected during the period of publication of Spam-Rankings.net daily outgoing spam data from the Composite Blocking List (CBL) on 15,657 ASNs in 205 countries and areas all over the world.

TABLE I
DISTRIBUTION OF SPAMMING ASNS ACROSS COUNTRIES

Number of spamming ASNs	Number of countries
>100	29
>50	17
>10	48
Subtotal	94
≤10	111
Total	205

The United States has the largest number (3,815) of ASNs, followed by Russia (1,828) and Ukraine (836). Table I contains statistics on the distribution of observed ASNs among countries. We can see that the distribution is highly skewed that over 80 percent of spamming ASNs are scattered within 29 countries, which is only a seventh of the countries.

TABLE II
SUMMARY STATISTICS OF OUTGOING SPAM

Month	Mean	Standard deviation	Min	Max	Spamming ASNs
2011/3	206724	2126080	0	99234107	10549
2011/4	166141	2028394	0	140284540	10126
2011/5	104488	1449672	0	131120382	9711
2011/6	121775	1645372	0	137096653	9782
2011/7	103156	1424145	0	97963663	9126
2011/8	95332	1351760	0	84812377	8994
2011/9	123115	1712561	0	92128338	8901
2011/10	108914	1543344	0	95194625	9003
2011/11	66179	934372	0	64111728	9304
2011/12	61714	776539	0	41208814	9376
2012/1	71010	929679	0	45787666	9033
2012/2	65372	750438	0	33701736	9478
2012/3	58193	667938	0	33881560	9573
2012/4	54276	702873	0	36967993	9320
2012/5	53450	782549	0	50504031	9451
2012/6	42640	662836	0	48523440	9165
2012/7	37563	766878	0	73802240	9221

The outgoing spam volume data show that the distribution spam volume is also skewed that a small portion of ASNs sent out most of the spam. Table II presents the summary statistics of outgoing spam by ASN. It shows that the standard deviation of outgoing spam volume among ASNs is over 10 times of the

average volume. We can also see a decreasing trend in average outgoing spam volume over time since the beginning of this project while the number of ASNs with positive outgoing spam volume is relatively stable.

D. Interventions

Our treatments may be considered analogous to those used in a recent immunization study of children in India [16], in which the individual participants were 1640 children clustered as follows:

> Interventions 134 villages were randomised to one of three groups: a once monthly reliable immunisation camp (intervention A; 379 children from 30 villages); a once monthly reliable immunisation camp with small incentives (raw lentils and metal plates for completed immunisation; intervention B; 382 children from 30 villages), or control (no intervention, 860 children in 74 villages). Surveys were undertaken in randomly selected households at baseline and about 18 months after the interventions started (end point).

Similarly to the immunization study, we propose three groups: just publish rankings; publish and aggressively publicise and contact ranked organizations; and don't publish about the control group.

Indeed, all the Indian children were in the one Indian state of Rajasthan, but all ASNs are on the same Internet.

E. Study and evaluation design

Using data underlying the published and unpublished rankings, we regressed outgoing spam volume on its lag, and found that the spam volume in last month explains about 85% of the variation in spam volume. Variation between countries only accounts for less than 2% of the total variation. A power analysis was conducted using the design approach for a cluster randomized trial in the software of Optimal Design. The results show that in order to achieve a power of 80%, if we can get at least 50 ASNs within each country, we need to have at least 20 countries if we take into account the influence of last period spam volume or 40 countries if not. If we can get at least 100 ASNs within each country, we only need to have 12 countries if we take into account the influence of last period spam volume or 28 countries if not. According to Table I, our current sample set can support our basic experiment.

F. Methods of publicity

If we propose to select countries from throughout the whole world, with a variety of geographies, legal regimes, and languages, how do we propose to make the SpamRankings.net website known in all those countries?

We do it using the Internet and through other means such as technical organizations. For example, every ISP in the European region is a member of RIPE and has technical people going to RIPE conferences. Similarly for APNIC in the Asia-Pacific region, LACNIC in Latin America and the Caribbean, AfriNIC in Africa, and ARIN in North America (which usually meets same time and place as NANOG, the North American Operator's Group). We have already presented at one NANOG [24] and one RIPE [25] conference, as well as at invited operational [26] and security [5] workshops, and we will present at more. The Anti-Phishing Working Group (APWG) draws technical, legal, and political people from the entire world; one of us has presented at the eCrime conference APWG co-organizes [27], [28]. Other relevant worldwide organizations include Messaging Anti-Abuse Working Group (MAAWG).

And it's not just ISPs. Look at the medical organizations. All of the high-ranking ones dropped to zero at the same time because they all talk to each other [29]. Even the last chronic holdout, WIN, finally fell out of the lead, even though it's based in Belgium and the rest are mostly in U.S., Canada, and Korea [30].

The Internet is global, and technical security people in every type of organization worldwide are part of the same community. The common language of that community is English. Certainly most Internet security participants probably use their local languages day to day, but all of them have access to English-reading and -speaking colleagues.

Their corporate executives may be somewhat more insular, but the worldwide economy is also integrated, as is the global press. In addition to trade blogs [31] and magazines [32], we use global publications such as Network World [33], CACM [34], Economist, Financial Times, etc. as often as we can get covered.

Finally, the Internet itself will be a direct conduit to some types of treatment. We already publish frequent updates on the website and make notifications of them readily available through an RSS feed, http://feeds.feedburner.com/Spamrankingsnet, plus a Wordpress widget, http://www.spamrankings.net/widget/. We will be adding twitter, facebook, and YouTube postings.

It is also possible to use contact information found on the websites of ranked organizations to inform them that they are ranked, no matter where they are in the world.

G. Data sources

The most important point about our data sources is that this is not a survey-based project. We get data every day about ASNs in every country in the world that sends out significant amounts of spam. The public SpamRankings.net uses no data collected from the ranked companies themselves.

1) Spam as a sneeze for infosec disease: To conduct the field experiment, we need data available now with which to build reputational rankings. Fortunately, spam is a sneeze for infosec disease, and anti-spam blocklists provide us copious data on spam, with which we have already prototyped SpamRankings.net. Outgoing spam is a proxy for Internet security because it could be a symptom of far more damaging security problems like malware, [5]. Spam is typically generated via zombie computers, compromised user accounts, or spammers who knowingly abuse their accounts. Spammers can steal existing accounts by tricking end-users into providing their

email usernames and passwords. Computers infected with malware often send spam as part of a botnet. If a computer is under the control of a malicious third party, it could lead to problems such as theft of customer records and intellectual property, fraudulent use of corporate online banking, and even employee blackmail.

Because bot herders will attack any computer that can send email, spam can come from any Electronic Mail Service Provider (ESP) on the Internet, not just Internet Service Providers (ISPs), so blocklists provide us data on the entire Internet. ESPs are constantly fighting against inbound spam, phishing and email-borne malware. Internal costs of outbound spam include IP blocking by RBL, DNSBL, and IP reputation systems, causing queue buildup on the affected mail server, delays in message delivery, and may result in lost messages and calls from unhappy end-users. It also leads to compromised user accounts and blocking of legitimate outbound email.

ESPs may not be aware that they are a source of malicious emails. ESP users also do not know unless a serious attack happens. Thus an ESP user sending spam not only risks being attacked but also increases risks for other users. Eventually, outbound spam could mean damaged reputation, customer dissatisfaction, increased operational costs, and loss of potential profit.

2) Blocklists collected: Any infosec metric source will find some problems and overlook some that other metrics might find [35]. For this reason, we use multiple anti-spam blocklists.

SpamRankings.net derives its current rankings from two blocklists: CBL (Composite Blocking List) and PSBL (Passive Spam Blocklist). (CBL is also the main component of Spamhaus' XBL.) In addition to their standard lists of IP addresses, CBL and PSBL send us additional custom data: volume information (numbers of spam messages seen from each IP address). CBL also sends us for each address the latest botnet (if any) they detected for that address.

CBL sends us data on millions of spam messages a day. While this is only a fraction of daily spam Internet spam, it is a large enough sample to compare organizations over time.

Each blocklist uses different spam traps and other sources, each with its own biases. Each has its own methods of determining which email messages to consider spam. Yet the various blocklists do see quite similar views of large-scale spam characteristics of the Internet, as we determined before we started publishing rankings [36]. We continue to compare CBL and PSBL results as we publish rankings.

We also collect daily data four other blocklists plus several specialized sources, all available for further rankings.

3) Data aggregation: We aggregate blocklist information per netblock and then per Autonomous System Number (ASN), and soon per organization, taking account of overlaps at each step so as not double-count volume. We also record further custom data such as the botnet and other source type information CBL sends us (snowshoe, darkmailer, etc.). We manually add categorization attributes per organization, such as Educational, Hosting, ISP, Medical, or Financial, plus finer detail such as services offered.

We have performed statistical analyses at the IP address level and at the ASN level regarding rapidity of detection, growth of volume, recidivism, and the like, including per category [37]. A large proportion of the technical infrastructure hours spent on the project is dedicated to data integrity.

4) Ranking levels: The data lends itself to aggregation at several Internet technical levels, most prominently netblock, ASN, and owning organization. Other levels that could be constructed might include states within countries, Metropolitan Statistical Areas (MSAs), or cities: all of those more detailed geographical levels would require adding more detailed geographical localization data, and would have the drawbacks of diminishing amounts of spam discussed in §*II-A Geographical scope and unit size*.

We are currently publishing rankings mainly at the ASN level. However, we are exploring arguments for perhaps publishing rankings at the netblock level because for example the constituent part of Microsoft's AS 8075 that caused it to appear many times at the top of one ranking [33], was mostly a netblock for Hotmail.

Rankings by netblock would produce more units, and thus make for easier and perhaps more robust statistics. However, for many organizations there won't be much difference per netblock, but for larger ones there will be, especially big corporations with many divisions.

Similarly, many organizations have only one ASN (and some have none), but some organizations (especially those that have formed by merging from previous organizations) have many. Big ISPs and companies like google are examples. Their acquisitions still use their old ASNs, and many of the customers of those acquisitions may think of YouTube or UUNET with identities separate from their new parent companies.

In addition, ISPs often put cable or DSL rotary addresses on their own netblocks, and those are used by different classes of customers than the netblocks or ASNs supporting their VPN services.

We could publicize rankings at all three levels (organization, ASN, and netblock), but that would make it difficult to disentangle the effects treatments at each level. We could let some groups receive one level ranking and some another level.

We actually already publish rankings at three levels: Countries in the world, and ASNs per country, and ASNs in an organizational category (medical) that crosses country boundaries.

The idea of the experiment is to get different groups receiving different information so that we can validate our theory and hypotheses through comparison results. Currently, we have industry ranking and country ranking, which is used in order to test if industry ranking can better incentivize companies than country ranking so that we can support our hypothesis of peer influence.

5) Data presentation: The current model for the public SpamRankings.net is sports scores: tables with rows of rank, team (ASN), and score (spam volume). In addition we provide bar and pie charts of monthly data, plus a line graph of daily

data, in both linear and logarithmic form.

Each ranking is currently derived from a single blocklist for ready comparison. We plan various forms of normalized and derivative rankings. Perhaps most importantly, we plan to add composite rankings that distill various other rankings into summaries.

Perhaps the most important features of the public rankings are the groupings of ASNs into rankings. Currently we are publishing groupings mostly by country, with a few also by organizational type (medical).

The experiments largely involve varying the degree of publicity of the rankings. Rankings in the control group will not be published (but will be visible internally to researchers). One treatment group of rankings will be published much like the ones currently visible on SpamRankings.net. A second treatment group will be published and will also be actively publicized through various means.

H. End points

Our data and treatments are somewhat different from the usual relatively brief medical treatments with definite end points. For example, the Indian immunization study was about immunization of children with vaccines, and naturally came to an end point once the vaccinating medical personnel had finished their injection work [16]. Our data come in regularly daily, and the treatments can continue as long as we like. For SpamRankings.net itself, currently rankings are published monthly, so one could consider every month's publication of a ranking as an end point.

I. Costs

Which infosec actually works best against which exploits and attacks? As Dr. Dan Geer reminds us [38]:

> Do you think our enemies will hesitate to spend $1,000 to attack a target? Do you think they'll hesitate to spend $10,000? We don't. We aren't smarter than the TSA. We can't win this spending game. So what's the path out of these woods? We don't know, but we do know this: whatever it is, it'll involve us spending money on a smaller number of things. An asymmetric enemy makes us spend a dollar on every single thing that might happen while he spends money on the one thing that will happen, and that's a mug's game.

The current experiments may not address this question directly, but they do make visible which organizations are not coping sufficiently with at least one type of asymmetric enemy, namely spammers, and, more importantly, with the underlying vulnerabilities and exploits that make spamming possible and also enable other possible exploits, such as identity theft, blackmail, or DDoS. They also set the stage for examining which infosec works best; see below under future experiments.

J. Drilldown

Simple observation that they are ranked can be enough for many organizations to know what to do to get out of that ranking. Others contact us for assistance.

Project researchers can use unpublished rankings in comparisons, as well as internal drilldown interfaces (some used in this paper) to specific ASNs, netblocks, and botnets, with adjustable timeframes [1]. For example, we can see which botnets appear to be infesting a given ASN, and we can tell which ASNs seem to be infested by a given botnet.

Other issues we are currently using drilldowns to investigate include the snowshoe spam swelling this year and spreading beyond its normal hosting center loci into ISPs and into countries other than the U.S. [21], the recent Grum takedown by FireEye [22], and the sudden surge of Festi spam around the world, which has pushed India to the top of the world rankings and put Saudi Arabia and Turkey in the top 10 spamming countries [23].

In addition to the three technical levels of grouping already discussed (organization, ASN, and netblock), there is also the fourth level, of individual IP address. That level is important along with the netblock level for drilldowns to satisfy inquiries from ranked organizations. Publishing rankings on individual IP addresses would probably not be very productive, since there are so many of them, although for drilldowns we may produce displays for individual IP addresses similar to those for rankings.

For drilldowns it would be useful to find a way to make a statistical connection between observed performance at the ASN or netblock level and the individual IP address level [37].

III. Discussion

A. Preliminary Results

Even before publishing SpamRankings.net, we determined some preliminary results, including that most ESPs do not ever send spam; some always do; size matters (the bigger the ESP, the more likely it spams); and some do migrate between the two groups. Partitions of providers already exist in the field: national and state telecommunication companies are the worst, sending much of total spam worldwide, [5].

1) Medical: When we started publishing SpamRankings.net in May 2011, we included a pair of rankings (from CBL and PSBL data) for medical organizations. Soon afterwards, they almost all dropped all together to zero spam volume [39] from both blocklists. A technical contact at one of the suddenly-improved hospitals told us they had found and fixed their immediate problem, and:

> "The listing on your site added additional impetus to make sure we "stay clean" so in that regard, you are successful."

He further indicated that all the big medical organizations talked to each other all the time, and he indicated that they might be adding some further infosec to ensure future cleanliness. The same anonymous contact recently revealed further detail to a Network World reporter [33].

A year into publishing SpamRankings.net, overall spam from medical organizations remains low, and usually when one of them gets ranked, it vanishes again next month [29]. The one recidivist holdout, WIN's AS 9208, finally started

decreasing its volume in March 2012 and dropped out of the July 2012 CBL top 10 ranking [30].

2) Microsoft: After Microsoft's AS 8075 topped the U.S. SpamRankings.net from PSBL for the fourth time, [40], we sent inquiries to some Microsoft contacts, but heard nothing back. After the fifth time, Network World wrote about it [33]. That same day we were contacted by two people from Microsoft. Examining the specific IP addresses observed by PSBL as sending the spam, we noticed that about 3/4 of them were associated with Hotmail. This is an example of how publicity does get attention to the rankings. We are watching to see whether AS 8075 drops in the rankings. So far, volume is lower, but it may decrease further.

This ASN only topped the PSBL U.S. rankings; it never appeared in the U.S. top 10 from CBL data. This example illustrates that differing results from different data sources is not a bug: it is a feature.

3) Takedowns: Takedowns and blocklists do temporarily reduce spam from specific ESPs, as in the shutdown of Triple Fiber Network [41] or FireEye's takedown of the Ozdok botnet [24]. However, such effects are indeed temporary; see below under Drilldown. the Grum botnet [22].

4) Other: A statistical analysis (submitted for publication elsewhere) of country rankings, comparing the publicly presented ones to other rankings internally visible to researchers, indicates publication does affect organizational behavior.

B. Comparison with other studies

The Collaborative Center for Internet Epidemiology and Defenses (CCIED) [42] does excellent work such as on new methods of spam filtering [43]. Other organizations such as Georgia Tech also study filtering methods [44]. Our project does not study how specific infosec works, although we may use results of such studies for infosec effectiveness experiments.

Many interesting studies of spam and other malware used logs or survey responses from affected organizations [45], [46]. Our data sources do not require cooperation of the ranked organizations, providing some independence from deliberate organizational bias.

Internet security professionals are starting to recognize that security metrics are required to replace fear, uncertainty, and doubt in the Internet, [47], but to date while metrics have been deployed extensively within organizations, [48], the ignored elephant in the room remains "the necessity of comparative analytics" across organizations, [49].

Many previous studies were mostly limited to Internet Service Providers (ISPs) [50], [51]. Since our sources are anti-spam blocklists (and eventually also APWG's phishing report database), our rankings can cover every organization on the Internet that spams or phishes.

C. Limitations of study

While our data set is as complete as possible, any data source is going to be incomplete. The next question is how the incompleteness of the data we receive will be handled within the experiment. We already provide acknowledgment of the sources of the information, and we do and will provide descriptions of our processing of the data so that the limitations of the data are acknowledged. The primary question our experiment is designed to answer is is not whether or not the information is noisy: all available information in this regard is obviously noisy. Rather the question we ask is whether making this information public – despite its limitations – can be an effective tool to encourage companies to change their infosec.

Three points often come up in discussions of country-level randomization. Here they are, with responses to each.

1) The units of randomization are very heterogeneous.
   Yet, as we noted above in §*II-E Study and evaluation design*, "Variation between countries only accounts for less than 2% of the total variation."
2) There are not very many of them.
   Many clustered RCTs use fewer units than we have available. As we noted above in §*II-E Study and evaluation design*, we have enough country units to achieve a power of 80%.
3) Our ability to collect information might vary significantly by country.
   This item usually results from a misunderstanding of the nature of our data. We do not go out and collect our data in surveys. We do not depend on cooperation of the subject organizations to provide data. The subject organizations send outbound spam, anti-spam blocklists collect it, and some of those blocklists send us the data we use. An organization cannot refuse to cooperate with a survey, because there is no survey. The only way an organization can refuse to cooperate is by not sending outbound spam. That would indeed improve an organization's rankings, and would be a positive effect of the rankings and of the experiments.
   As we noted in *II.C. Selection and description of sample*, we see significant events in countries such as Saudi Arabia and Turkey in which we are relatively certain none of the blocklists that send us data have spamtraps. Actually, a huge advantage of the data used in this project is that we can see every country in the world, on a daily basis, in some detail, with metrics that are comparable across countries.

We are continually trying various approaches, including different geographic and other levels of ranking and randomization, and we always value input.

D. Policy implications

Our principal objective is to demonstrate that requiring firms to report on their Internet security issues can enable solutions for improved Internet security, especially when combined with reputational rankings for visiblility of peer comparisons. A mandatory reporting policy can induce positive reaction from firms so that they would have improved security awareness, vulnerability detection, and information protection.

We propose to leverage mechanisms including (but not limited to): concerns for security breaches, sense of shame

or fame, and peer influence.

1) We hypothesize that that mandatory regular infosec reporting could force firms to take closer look at their security situation. We can test that hypothesis using data that is already publicly available, namely outbound spam, which does not need mandatory reporting, since anti-spam blocklists already detect it. SpamRankings.net correlates that data per organization, geography, category, etc. to produce public rankings for peer pressure. The policy implications can be applied to other security issues, where mandatory reporting could make comparable data available. Simply having to report would increase firms' awareness their security vulnerabilities, potentially costing reputation and profit through third party exploits.
2) Publicizing their security issues can make firms feel ashamed of their irresponsibility for others' Internet security. Shame is triggered by a choice made in public that does not maximize the payoffs of others, [52]. [53] argue that a person's behavior may depend on whether it is observed by someone who is directly affected by it. A classic dictator game is where one person gets to anonymously divide some money (usually $10) between herself and another person, [54]. Many studies use a variant of the dictator game, where the dictator can opt out the game before the recipient learns it is being played. The dictator can get a pre-specified amount of money if she exits, and the recipient gets nothing. It turns out one third of the participants choose to exit when offered $9, [55]. If the dictator is completely altruistic, playing the game and choosing $9 for herself and $1 for the recipient would be a preferred choice. If the dictator is completely selfish, playing the game and allocating all $10 to herself would be preferred. Therefore, [53] develop the concept of moral cost (shame) that enters the utility function additively to justify such behavior. The effect of observation on the agent's behavior can be extended to organizations because organizations are concerned about their social image and performance, [56]. Conversely, every ISP thinks it is the best in the world at what it does. Rankings based on real data could provide some of them (and other ESPs) with evidence and help publicizing such infosec fame, attracting or retaining customers increasingly concerned with privacy and confidentiality.
3) The last and also the most important incentive for organizations to take positive reaction is peer influence through explicitly comparing each organization to others. Social comparison theory, [57], indicates that publicly comparing similar organizations can change their behavior through peer pressure, [58] demonstrates that, after controlling for an individual's own income, higher earnings of neighbors are associated with lower levels self-reported happiness. This finding proves that individuals care about their relative position in comparisons. For organizations, we expect peer pressure to be more prominent because similar businesses would compete in the same market on the same group of customers, [59]. Rankings derived from the data mobilized by mandatory breach reporting would put peer pressure on organizations to improve their infosec, and would also make visible what kinds of exploits were successful so white hat security personnel could fight them better.

SpamRankings.net focuses on outbound spam because that data is readily available through anti-spam blocklists. If this reputational approach proves out through experiment, applying it to other data would be appropriate.

The Anti-Spam Working Group (APWG) collects a large database of phishing reports and makes it available to researchers. We are familiar [27] with that database's problems of coverage [60]. However, we have plans to produce two sets of phishing organizational rankings (senders of phishing message and hosters of phishing websites). We do not plan to use those phishing rankings standalone, nor do we expect them to completely measure phishing, anymore than we expect our spam rankings to completely measure spam. Like for the spam data, we expect the phishing data to provide indications. We expect the phishing rankings to be especially useful in comparison to the spam rankings, to observe how changes in one symptom of poor infosec (spam) for organizations are reflected in changes in another symptom (phishing). Spamming botnets do not normally also send phishing messages, so coordinated changes in phishing and spam rankings for an organization would be evidence of changes in its underlying infosec. Conversely, if an organization drops on one kind of ranking (phishing or spam) but not on the other, it would seem to still have an infosec problem. This is one way we can determine how much changes in the spam rankings actually indicate changes in underlying infosec.

Other available data sources include Dshield [61] and the National Vulnerability Database (NVD) [62]. Such data sources also be used to calibrate the spam data, although their utility is limited, because those datasets are not updated very often and are not very comprehensive.

Governments or trade associations or stock markets could require infosec problem disclosure publicly through the Internet. Such data could enable more rankings for more incentives.

Traditional government, being slow and geographically organized, cannot handle the rapidly changing miscreant economy that fuels worldwide spam. Private parties alone have clearly failed to do so. What is needed is the kind of multi-level multi-organizational loose cooperation that studies of governance of many types of commons indicate works [63]. The key feature is "management by the users themselves," [64].

> The reliability and security of the Internet, however, is a public good that cannot be ignored. The security of the Internet is a public good because availability to one user does not diminish its availability to another user.
> ...in large and complex systems, there should be

> multiple layers of nested enterprises (p. 101 f). In the case of the Internet, individual users operate at a low level, while organizations and user communities operate at a middle level.

Contribution to the public good can be effectively encouraged by "rewards for those with a good reputation in the public goods game" [65]. Rankings such as pioneered by SpamRankings.net and studied with the experiments outlined in this paper can provide information and incentive for stakeholders to organize themselves to collectively manage the Internet commons [63].

The importance of infosec is increasing as the entire world becomes increasingly dependent on computers and networks [66]. As Dr. Geer reminded us [67],

> Attacking national infrastructures is also done with computers – often hijacked computers. Thus, threats to computing infrastructures are explicitly and inherently risk harm to those very societies in proportion to those society's dependence on them.

The Pentagon now considers cyber attacks from a foreign nation as an "act of war", [68].

The policy implications of this work thus conceivably extend to societal and national security.

E. Interpretation, unanswered questions, and future research

We can do multiple rankings as still more treatments (rankings from 2+ blocklists, normalized by country population, by Internet users per country; recidivism, resistance; monthly, weekly, daily; etc.). Such multiple rankings could permit doing multiple field trials using the same countries, since ASNs would rank differently for each ranking, and some that didn't appear at all in one ranking might be at the top of another ranking. See for example Microsoft appearing at the top of the U.S. PSBL ranking, while not appearing at all ever in the U.S. CBL ranking.

The multiple vaccines accounted for in the immunization study [16] might be considered analogous to multiple rankings.

Conversely, those vaccines might be considered analogous to different infosec applied by the ranked organizations, with our treatments being publicization of rankings by infosec. We have sketched out methods of distinguishing infosec so as to determine which infosec works, perhaps even which infosec works against which exploits.

IV. Conclusion

Reputation derived from publishing comparisons of infosec symptoms apparently do cause changes in infosec of ranked organizations. This project builds on promising pilot studies, moving to systematic experiments with statistical examination. If those more rigorous trials are successful, they will motivate policy recommendations for further infosec disclosure, enabling further reputational rankings and more improved infosec.

Biography

Leigh L. Linden is an Assistant Professor in the Department of Economics at the University of Texas at Austin with a joint appointment in the Lyndon B. Johnson School of Public Affairs. He earned a PhD in Economics from MIT in 2004 and received a Bachelor of Science in Mathematics and a Bachelor of Arts in Economics from the University of Texas at Austin in 1997. He specializes in the use of large-scale randomized controlled trials. His research has been published in the American Economic Review, the Quarterly Journal of Economics, and the Applied Economic Journal: Applied Economics. It has also been featured in several popular press publications including The New York Times, The Washington Post, The Economist, The Financial Times, and The Christian Science Monitor. He is affiliated with the National Bureau of Economic Research (NBER) and the Bureau for Research and Economic Analysis of Development (BREAD).

John S. Quarterman worked for BBN, the prime contractor on the ARPANET, in the early days of the Internet. He is currently Principal of Quarterman Creations and CEO of InternetPerils, Inc., an Internet business risk management intelligence agency that provides automated quantification and visualization products. He founded the first Internet consulting firm in Texas. He founded one of the first local ISPs in Texas and sold it at a profit. He founded the first Internet performance metrics company in the world, which drew the first maps of the Internet, and which received substantial venture capital investment. He is the author of seven books related to the Internet, as well as numerous articles, presentations, and patents.

Qian Tang is a Ph.D. student in the Information, Risk, and Operation Management Department at the McCombs School of Business at the University of Texas at Austin. She received a Master of Science in Management in 2008 and a Bachelor of Business Administration in 2006 from Tsinghua University in Beijing, China.

Andrew B. Whinston received his Ph.D. at CarnegieMellon University and is currently a professor at The University of Texas at Austin where he holds the Hugh Roy Cullen Centennial Chair in Business Administration and is the director of the Center for Research in Electronic Commerce. He has published extensively on resource allocation issues and is currently working on Internet security. He has completed numerous research projects that investigate economics, Internet technology, and operations research in the study of information systems issues. In 2011 he was rated as the most influential scholar in the Information Systems field by the h-index which measures scholarly influence.

Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant No. 0831338. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

We also gratefully acknowledge custom data from CBL, PSBL, the University of Texas Computer Science Department, Quarterman Creations, and especially Team Cymru. None of them are responsible for anything we do, either.

REFERENCES

[1] J. S. Quarterman, S. Sayin, and A. B. Whinston, "Rustock botnet and asns," in *TPRC 2011*. TPRC, September 2011.

[2] C. Udry, "Esther duflo: 2010 john bates clark medalist," *Journal of Economic Perspectives*, vol. 25, no. 3, pp. 197–216, 2011.

[3] E. Duflo, R. Hanna, and S. P. Ryan, "Incentives work: Getting teachers to come to school," *American Economic Review*, May 2010, http://econ-www.mit.edu/files/5582.

[4] J. Menn, "A war marked by fatalism and denial," *Financial times*, November 2011.

[5] J. S. Quarterman, S. Sayin, M. Parameswaran, J. Reinikainen, and A. B. Whinston, "Spam reputation as output measure of infosec," in *Metricon 5.0*, August 2010, http://www.securitymetrics.org/content/attach/Metricon5.0/metricon5%20-%20quarterman%20-%20spam%20reputation.pdf.

[6] P. Manzano, "Enisa 2009 spam survey: Measures used by providers to reduce spam," *White Paper*, December 2009, http://www.enisa.europa.eu/act/res/other-areas/anti-spam-measures/studies/spam-survey.

[7] P. Herzog, "Better security through sacrificing maidens," *infosecisland*, August 2010, https://www.infosecisland.com/blogview/6646-Better-Security-Through-Sacrificing-Maidens.html.

[8] R. Anderson and T. Moore, "The economics of information security," *Science*, vol. 314, no. 610, pp. 610–613, 2006.

[9] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Transactions on Information and Systems Security*, vol. 5, no. 4, pp. 428–457, 2002.

[10] J. Quarterman, K. Harker, and P. Salus, "Combat power and enterprise competitiveness," *First Monday*, vol. 8, no. 1, January 2003, http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1022/943.

[11] M. Parameswaran and A. B. Whinston, *Incentive Mechanisms for Internet Security*. Emerald Group Publishing Limited, 2009, vol. 4, ch. 4.

[12] H. Xu, J. Chen, and A. B. Whinston, "Audited reputation," *Economics Letters*, vol. 100, no. 3, pp. 359–362, September 2008, http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6V84-4S0JMWP-1&_user=10&_coverDate=09%2F30%2F2008&_rdoc=1&_fmt=high&_orig=search&_origin=search&_sort=d&_docanchor=&view=c&_searchStrId=1456301194&_rerunOrigin=google&_acct=C000050221&_version=1&_urlVersion=0&_userid=10&md5=002dd3c652ebb96ce6eb905f70fb796a&searchtype=a.

[13] J. M. Bland, "Cluster randomised trials in the medical literature: two bibliometric surveys," *BMC*, August 2004, http://www.biomedcentral.com/1471-2288/4/21.

[14] R. Doughty, S. Wright, A. Pearl, H. Walsh, S. Muncaster, G. Whalley, G. Gamble, and N. Sharpe, "Randomized, controlled trial of integrated heart failure management. the auckland heart failure management study," *European Heart Journal*, vol. 23, pp. 139–146, March 2002, http://eurheartj.oxfordjournals.org/content/23/2/139.short.

[15] M. K. Campbell, D. R. Elbourne, and D. G. Altman, "Consort statement: extension to cluster randomised trials," *BMJ*, March 2004, http://www.bmj.com/content/328/7441/702.full.

[16] A. V. Banerjee, E. Duflo, R. Glennerster, and D. Kothari, "Improving immunisation coverage in rural india: clustered randomised controlled evaluation of immunisation campaigns with and without incentives," *BMJ*, May 2010, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2871989/.

[17] M. Bertrand, E. Duflo, and S. Mullainathan, "How much should we trust difference-in-differences estimates?" *Quarterly Journal of Economics*, vol. 119, no. 1, pp. 249–275, 2004.

[18] J. M. Wooldridge, "Cluster-sample methods in applied econometrics," *American Economic Review*, vol. 93, May 2003, http://ideas.repec.org/a/aea/aecrev/v93y2003i2p133-138.html.

[19] A. C. Cameron, J. B. Gelbach, and D. L. Miller, "Bootstrap-based improvements for inference with clustered errors," *The Review of Economics and Statistics*, vol. 90, 2008, http://www.mitpressjournals.org/doi/abs/10.1162/rest.90.3.414?journalCode=rest.

[20] A. V. Banerjee and E. Duflo, "Growth theory through the lens of development economics," *MIT Department of Economics Working Paper*, vol. 05, December 2004, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=651483.

[21] J. S. Quarterman, "Cdm snowshoes to the top of the world in may 2012 spamrankings.net," *Perilocity*, June 2012, http://riskman.typepad.com/perilocity/2012/06/cdm-snowshoes-to-the-top-of-the-world-in-may-2012-spamrankingsnet.html.

[22] ——, "Grum down, but... 1 june 2012 - 30 july 2012, spamrankings.net," *Perilocity*, July 2012, http://riskman.typepad.com/perilocity/2012/07/grum-down-but-1-june-2012-30-july-2012-spamrankingsnet.html.

[23] ——, "Festi botnet infesting the world, july 2012," *Perilocity*, August 2012, http://riskman.typepad.com/perilocity/2012/08/festi-botnet-infesting-the-world-july-2012.html.

[24] J. S. Quarterman and A. Whinston, "Fireeye's ozdok botnet takedown in spam blocklists and volume observed by iiar project," in *NANOG 48: Proceedings of the 48th North American Network Operators Group*, Feb 2010, http://www.nanog.org/meetings/nanog48/presentations/Wednesday/Quarterman_light_N48.pdf.

[25] J. S. Quarterman, A. B. Whinston, S. Sayin, E. V. Kumar, J. Reinikainen, and J. Ahlroth, "Transparency as incentive for internet security: Organizational layers for reputation," in *RIPE 61*. RIPE, November 2010, http://ripe61.ripe.net/presentations/116-Quarterman-presentation-Rome.pdf.

[26] J. S. Quarterman, S. Sayin, J. Reinikainen, E. V. Kumar, and A. B. Whinston, "Data, reputation, and certification against spam," in *DDCSW: Collaborative Data-Driven Security for High Performance Networks*. Internet2 and WUSTL, August 2010, http://security.internet2.edu/ddcsw2/docs/Quarterman-darepcert.pdf.

[27] J. S. Quarterman, "Phishscope: Tracking phish server clusters," in *APWG eCrime*, November 2006.

[28] J. S. Quarterman and A. B. Whinston, "Economic incentives for internet security through reputation and insurance," in *invitation-only first APWG and IEEE-SA Roadmapping Session, Toward a Global Public Health Initiative Model for eCrime Response*. APWG and IEEE-SA, October 2010, http://cism.mccombs.utexas.edu/iiar-project.

[29] J. S. Quarterman, "A year of spamrankings.net: Medical organizations," *RIPE Labs*, May 2012, https://labs.ripe.net/Members/jsq/a-year-of-medical-spamrankings.net-medical-organizations-1.

[30] ——, "Win finally got the no medical spam memo in march 2012," *Perilocity*, August 2012, http://riskman.typepad.com/perilocity/2012/08/win-finally-got-the-no-medical-spam-memo-in-march-2012.html.

[31] B. Krebs, "Naming & shaming sources of spam," *Krebs on Security*, June 2011, http://krebsonsecurity.com/2011/06/naming-shaming-sources-of-spam/.

[32] F. Y. Rashid, "Ut researchers launch spamrankings to flag hospitals hijacked by spammers," *eWeek.com*, June 2011.

[33] T. Greene, "Study: Microsoft repeatedly ranks as top u.s. spammer: University of texas project calls attention to problem in effort to reduce spam, improve security," *Network World*, July 2012, http://www.networkworld.com/news/2012/072512-microsoft-spammer-261183.html.

[34] S. Greengard, "How much spam does your company unknowingly send?" *CACM*, June 2011, http://cacm.acm.org/news/109807-how-much-spam-does-your-company-unknowingly-send/fulltext.

[35] M. V. Eeten, H. Asghari, J. M. Bauer, and S. Tabatabaie, "Internet service providers and botnet mitigation: A fact-finding study on the dutch market," *Report*, January 2011, http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/01/13/internet-service-providers-and-botnet-mitigation.html.

[36] J. S. Quarterman, A. B. Whinston, S. Sayin, E. V. Kumar, J. Reinikainen, and J. Ahlroth, "Asn ranking correlations between spam blocklists," *RIPE Labs*, December 2010, https://labs.ripe.net/Members/jsq/asn-ranking-correlations-between-spam-blocklist.

[37] S. Sayin, M. Parameswaran, J. S. Quarterman, and A. B. Whinston, "Analysis of spamming behavior at different aggregation levels and implications for it security," in *INFORMS 2010*, November 2010.

[38] J. Daniel E. Geer and B. Blakley, "Are you smarter than the tsa? (hint: No)," *IEEE Security and Privacy*, vol. 10, pp. 94–95, July/August 2012, http://www.computer.org/csdl/mags/sp/2012/04/msp2012040094-abs.html.

[39] J. S. Quarterman, A. B. Whinston, S. Sayin, and J. Reinikainen, "The big medical drop in spamrankings.net," *RIPE Labs*, August 2011.

[40] J. S. Quarterman, "Spam from microsoft's as 8075 april 2011-june 2012," *Perilocity*, July 2012, http://riskman.typepad.com/perilocity/2012/07/spam-from-microsofts-as-8075-april-2011-june-2012.html.

[41] J. S. Quarterman, M. Sammallahti, H. Rui, and A. B. Whinston, "Autonomous system blocklisting effects of triple fiber network shutdown," *CREC Technical Report*, July 2009.

[42] N. Weaver and V. Paxson, "A worst-case worm," in *The Third Annual Workshop on Economics and Information Security (WEIS04)*. Digital Technology Center, University of Minnesota, 2004.

[43] A. Pitsillidis, K. Levchenko, V. Paxson, C. Kreibich, Nicholas, Savage, and G. M. Voelker, "Botnet judo: Fighting spam with itself," in *NDSS 2010: Proceedings of the Network and IT Security Conference*, March 2010, http://cseweb.ucsd.edu/%7Evoelker/pubs/judo-ndss10.pdf.

[44] S. Hao, N. A. Syed, N. Feamster, A. G. Gray, and S. Krasser, "Detecting spammers with snare: Spatio-temporal network-level automatic reputation engine," in *USENIX Security Symposium*, 2009, http://www.gtnoise.net/papers/2009/hao:snare:usenix09.pdf.

[45] T. MOORE and R. CLAYTON, "The impact of public information on phishing attack and defense," *Communications & Strategies*, vol. 1, no. 81, pp. 45–68, 1st quart 2011, http://ideas.repec.org/a/idt/journl/cs8102.html.

[46] M. J. van Eeten and J. M. Bauer, "Economics of malware: Security decisions, incentives and externalities," *DSTI/DOC*, vol. 1, May 2008.

[47] A. Jaquith, *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. Addison-Wesley Professional, 2007.

[48] R. Seiersen, "Practical security metrics in the 4th dimension," in *Metricon 5.0*, August 2010, http://www.securitymetrics.org/content/attach/Metricon5.0/metricon5%20-%20seiersen%20-%20kaiser4d.ppt.

[49] A. Hutton, "Bridging risk modeling, threat modeling, and operational metrics with the veris framework," in *Metricon 5.0*, August 2010, http://www.securitymetrics.org/content/attach/Metricon5.0/metricon5%20-%20hutton%20-%20veris.pdf.

[50] M. van Eeten, J. M. Bauer, H. Asghari, S. Tabatabaie, and D. Rand, "The role of internet service providers in botnet mitigation: An empirical analysis based on spam data," in *The Ninth Workshop on the Economics of Information Security (WEIS 2010)*, June 2010.

[51] D. Wood and B. Rowe, "Assessing home internet users' demand for security: Will they pay isps?" in *Workshop on the Economics of Information Security*, June 2011.

[52] K. Saito, "Role conflict and choice: Shame, temptation, and justifications," *Working paper*, 2011.

[53] D. Dillenberger and P. Sadowski, "Ashamed to be selfish," *Theoretical Economics*, December 2010, forthcoming http://www.dklevine.com/archive/refs4661465000000001193.pdf.

[54] C. F. Camerer, *Behavioral Game Theory: Experiments in Strategic Interaction*. Princeton University Press, 2003.

[55] J. Dana, D. Cain, and R. Dawes, "What you don't know won't hurt me: costly (but quiet) exit in a dictator game," *Organizational Behavior and Human Decision Processes*, vol. 100, no. 2, pp. 193–201, 2006.

[56] H. Rui and A. Whinston, "Designing a social-broadcasting-based business intelligence system," *ACM Trans. Manage. Inf. Syst.*, vol. 2, pp. 22:1–22:19, Jan. 2012. [Online]. Available: http://doi.acm.org/10.1145/2070710.2070713

[57] L. Festinger, "A theory of social comparison processes," *Human Relations*, vol. 7, no. 2, pp. 117–140, 1954, http://www.soc.ucsb.edu/faculty/friedkin/Syllabi/Soc147/ATheoryofSocialComparisonProcesses.pdf.

[58] E. F. P. Luttmer, "Neighbors as negatives: Relative earnings and well-being," *The Quarterly Journal of Economics*, vol. 120, no. 3, pp. 963–1002, August 2005, http://www.nber.org/~luttmer/relative.pdf.

[59] S. Frei, "The security of end-user pcs an empirical analysis," in *DDCSW: Collaborative Data-Driven Security for High Performance Networks*. Internet2 and WUSTL, August 2010, http://security.internet2.edu/ddcsw2/docs/sfrei.pdf.

[60] T. Moore and R. Clayton, "The consequence of non-cooperation in the fight against phishing." in *Third APWG eCrime Researchers Summit*, 2008.

[61] S. I. S. Center, *Cooperative Network Security Community*. SANS, 2001, http://www.dshield.org/.

[62] NIST, *National Vulnerability Database*. NIST Computer Security Division, Information Technology Laboratory, 2011, http://nvd.nist.gov/.

[63] T. Dietz, E. Ostrom, and P. C. Stern, "The struggle to govern the commons," *Science*, vol. 302, no. 5652, December 2003.

[64] R. Axelrod, "Governing the cyber commons," *Review Symposium: Beyond the Tragedy of the Commons*, 2010, http://www-personal.umich.edu/~axe/.

[65] M. Milinski, D. Semmann, and H.-J. Krambeck, "Reputation helps solve the 'tragedy of the commons'," *Nature*, vol. 415, January 2002.

[66] mi2g, "Silently preparing for the 100 billion dollar cyber-catastrophe risk," *News Alert*, February 2004.

[67] D. Geer, C. P. Pfleeger, B. Schneier, J. S. Quarterman, P. Metzger, B. Bace, , and P. Gutmann, "Cyberinsecurity: The cost of monopoly," September 2003, http://cryptome.org/cyberinsecurity.htm.

[68] S. Gorman and J. E. Barnes, "Cyber combat: Act of war: Pentagon sets stage for u.s. to respond to computer sabotage with military force." *The Wall Street Journal*, May 2011.